UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	Docket No. 20-cr-40036-TSH
	)	
	)	***LEAVE TO FILE REDACTED MEMO***
VINCENT KIEJZO	)	***AND TO FILE EXHIBITS UNDER SEAL***
	)	***REQUESTED ON 10/18/21***

DEFENDANT'S OBJECTION TO DISCOVERY ORDER AND REQUEST FOR REVIEW BY DISTRICT COURT JUDGE

Defendant Vincent Kiejzo moves this Court, pursuant to Fed. R. Crim. P. 59(a) to review and reverse Magistrate Judge David Hennessy's written order denying his motion to compel discovery. Mr. Kiejzo respectfully submits that Magistrate Judge Hennessy's order denying Mr. Kiejzo's motion to compel discovery is erroneous and contrary to law. The requested discovery is material to the preparation of Mr. Kiejzo's defense, necessary for the preparation and litigation of pretrial motions, and casts doubt on the admissibility of evidence in the government's case-in-chief. Mr. Kiejzo is therefore entitled to the discovery under Fed. R. Crim. P. 16(a)(1)(E), Local Rule 116, and *Brady v. Maryland*, 373 U.S. 83, 87 (1963).

FACTUAL AND PROCEDURAL BACKGROUND[1]

Mr. Kiejzo is charged, via indictment, with one count of Possession of Child Pornography in violation of 18 U.S.C. § 2252(a)(5)(B). The evidence against Mr. Kiejzo stems from materials discovered in his home pursuant to a search warrant. The allegations made in the search warrant affidavit and information omitted from that affidavit form the basis of the current dispute.

[1] For the sake of brevity, Mr. Kiejzo refers this Court to his original motion to compel for a more complete recitation of the relevant factual background. The facts stated therein, and here, are based on the discovery provided thus far by the government.

On September 8, 2020, Homeland Security Investigations ("HSI") Special Agent Caitlin Moynihan submitted an application for a warrant to search Mr. Kiejzo's home. Agent Moynihan's affidavit alleged that there was probable cause to believe that a user of the internet account at Mr. Kiejzo's home had accessed, one time each on a single date in May 2019, two Tor hidden-services websites geared towards the sexual exploitation of minors. *See* Exhibit F, Affidavit of Special Agent Moynihan, ¶ 5. The affidavit stated that in June 2019, the computer server hosting those websites, which was located outside the United States, was seized by a foreign law enforcement agency ("FLA"). *Id*. at ¶ 15, 23. It further stated that in August 2019, an FLA notified U.S. law enforcement that a specific IP address was twice "used to access online child sexual abuse and exploitation material via … website[s] that the FLA named and described as Website[s] 2 [and 3]" on a specific date in May 2019, seventeen minutes apart. *Id*. at ¶ 31-32. According to Agent Moynihan, U.S. law enforcement subsequently identified the IP address and associated it with Mr. Kiejzo's father, who lived at the same address as Mr. Kiejzo. *Id*. at ¶ 39-47. Magistrate Judge David Hennessy granted the search warrant for Mr. Kiejzo's residence, including certain records, tangible items, computing devices, software, and storage media. The warrant was executed on September 9, 2020.

Following his indictment, Mr. Kiejzo, through undersigned counsel, submitted detailed and itemized requests for discovery on February 16, 2021. *See* Exhibit A, Discovery Letter, 2/16/21. On or about March 17 and 18, 2021, the government provided some responsive materials and answers to the defendant's first discovery letter and declined to provide responses to several other requests. *See* Exhibit B, Government Response, 3/17/21. On May 3, 2021, the defendant submitted a supplemental discovery letter to the government, requesting additional specific and detailed items of discovery and providing additional, more fulsome justifications for the previously denied

requests. *See* Exhibit C, Supplemental Discovery Letter. On July 2, 2021, at the government's request, counsel submitted a third supplemental discovery letter providing additional, more fulsome justifications for the requests outlined in the May 3 letter. *Id.* On or about July 9, 2021, the government provided few responsive materials and answers to the defendant's discovery letters and declined to provide responses to several other requests. *See* Exhibit D, Government Response. Mr. Kiejzo then filed a motion to compel, under seal, on July 28, 2021. D.E. 80.

Through the discovery process, the government has provided scant details regarding the allegations made in the affidavit. Relevant to this motion, the government has identified the FLA that provided the tip notifying U.S. law enforcement that a particular IP "accessed child sexual abuse material" as [redacted] *See* Exhibit B at 2. The government also produced five pages of heavily redacted documents related to the tip. *See* Exhibits G-I. After Mr. Kiejzo filed his motion to compel, the government produced two new critical pieces of information.[2] First, the government stated that the server hosting Websites 2 and 3 was located in a country that is neither the United States nor [redacted] and that the FLA that seized the server is local to the server host country. *See* Exhibit L, Hearing Transcript, 8. Second, the government stated that FBI and HSI agents do know what country the server was located in and that it is neither the United States nor [redacted]. *See id*.

A hearing was held on Mr. Kiejzo's motion on September 17, 2021. The motion was ultimately denied, and Mr. Kiejzo was served with a copy of the Magistrate's order on October 4, 2021. D.E. 106.

[2] The government first produced this information to counsel via telephone prior to the motion hearing, and then again via email after the hearing.

LEGAL STANDARDS

Under Fed. R. Crim. P. 59(a), a district court must "consider timely objections and modify or set aside any part of [a magistrate judge's] order that is contrary to law or clearly erroneous." *See also* 28 U.S.C. § 636(b)(1)(a) ("A judge of the court may reconsider any pretrial matter … where it has been shown that the magistrate judge's order is clearly erroneous or contrary to law."). The party objecting to a magistrate's order must file objections within 14 days of being served a copy of the written order. Fed. R. Crim. P. 59(a).

Fed. R. Crim. P. 16(a)(1)(E) requires the government, upon the defendant's request, to turn over any item within the government's possession, custody, or control that (i) is material to preparing the defense, (ii) the government intends to use in its case-in-chief, or (iii) was obtained from or belongs to the defendant. The First Circuit has noted that "materiality" requires "*some indication* that pretrial disclosure of the information sought would have enabled the defendant significantly to alter the quantum of proof in his favor." *United States v. Goris*, 876 F.3d 40, 45 (1st Cir. 2017) (emphasis added). A "significant alteration may take place in a myriad of ways, such as uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." *Id*.

Local Rule 116 outlines the government's discovery responsibilities in more detail. Relevant to this motion, Local Rule 116.1 reaffirms that the government must fulfill its discovery obligations under Fed. R. Crim. P. 16(a)(1). Local Rule 116.2 goes further and requires the government to produce exculpatory evidence, which includes, but is not limited to information that "tends to (1) cast doubt on defendant's guilt as to any essential element in … the indictment … (2) cast doubt on the admissibility of evidence that the government anticipates using in its case-in-chief, that might be subject to a motion to suppress or exclude … (3) cast doubt on the credibility

or accuracy of any evidence that the government anticipates using in its case-in-chief." This rule implements *Brady v. Maryland*, 373 U.S. 83, 87 (1963), in which the Supreme Court held that the failure to disclose exculpatory evidence is a violation of due process.

In *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978), the Supreme Court held that a defendant is entitled to a hearing to challenge the truthfulness of statements in a search warrant affidavit if he makes "a substantial preliminary showing" that the statements were "knowingly and intentionally [false], or made with reckless disregard for the truth," and that the falsehood was "necessary to the finding of probable cause." Some courts have indicated that the same standard is required in order to obtain discovery to mount a *Franks* challenge. *See, e.g.*, *United States v. Long*, 774 F.3d 653, 661-62 (10th Cir. 2014) (where defendant sought disclosure of the name and contact information of a confidential informant in order "to obtain evidence for a *Franks* hearing," the Court upheld denied of that request because the defendant "did not make an adequate evidentiary showing under *Franks*").

However, at least one court in this district has acknowledged the difficult, if not impossible, burden that rests with the defendant when the *Franks* discovery sought relates to a confidential source. *See United States v. Jordan*, No. 09-10139-JLT, 2010 WL 625280, at *3 (D. Mass. Feb. 23, 2010) ("the courts recognize that when an affidavit relies primarily on information provided by a [confidential informant], a defendant will lack the information needed to make a *Franks* showing.") (*citing United States v. Manning*, 79 F.3d 212, 220 (1st Cir. 1996)). That court held – in the context of a defendant who sought information about a confidential informant – that the production of discovery related to a *Franks* challenge "should await an initial showing, at a minimum, that there are inaccuracies in the affidavit and that if the challenged information is omitted, there is no probable cause for the warrant." *Jordan*, 2010 WL 625280, at *4.

ARGUMENT

The requested items outlined below are discoverable under Rule 16(a)(1)(E) because: (1) Mr. Kiejzo has requested them, (2) the items are in the Government's possession, custody, or control, and (3) the items are material to the preparation of Mr. Kiejzo's defense. *See* Fed. R. Crim. P. 16(a)(1)(E). The information sought by Mr. Kiejzo is exculpatory, as it casts doubt on the accuracy of the information in the search warrant and therefore goes directly to the "admissibility of evidence the government anticipates offering in its case-in-chief." Local Rule 116.2(a); *Brady*, 373 U.S. at 87. The requested discovery must also be turned over because Mr. Kiejzo has made an initial showing that there are inaccuracies in the affidavit and that if those inaccuracies are corrected, and if omitted information is added to the affidavit, probable cause to search Mr. Kiejzo's home is absent. *Franks*, 438 U.S. at 155-56. This initial showing entitles Mr. Kiejzo to further discovery that is material to a *Franks* motion and his motion to suppress. The Magistrate Judge's findings to the contrary were erroneous and contrary to law and should be reversed by this Court pursuant to Fed. R. Crim. P. 59(a).

> ***Discovery Requests #3-4***[3]*: The identity of the FLA that seized the computer server hosting Websites 2 and 3 in June 2019, as referenced in ¶¶ 15-16 of the Affidavit.*

The government states that neither Target Website 2 nor 3 were hosted in the United States and that the computer server hosting these websites was located and seized by another FLA outside of the U.S., distinct from [redacted]. *See* Exhibit D; Exhibit L at 8. In discussion and correspondence with the Assistant United States Attorney, the defense learned that the FLA that seized the server is local to the server host country – again, distinct from [redacted]. Furthermore, the government has stated that the FBI and HSI agents know what the host country is and that it is

[3] The discovery items are numbered as they were in the defendant's discovery letters, at Exhibits A and C. Mr. Kiejzo reserves the right to request and obtain additional discovery beyond the categories herein.

neither the United States nor [redacted]. Despite the government's affirmative obligation to learn of and disclose this type of evidence, *see Kyles v. Whitley*, 514 U.S. 419, 437 (1995), it has declined to identify the FLA that seized the server.

The Magistrate's denial of Mr. Kiejzo's motion to compel this discovery was erroneous and contrary to law. Fed. R. Crim. P. 59(a). The standard is not whether a "defendant can prosecute a motion to suppress" without the requested information. *See* Exhibit N, Magistrate Judge's Order Denying Motion to Compel, 6. Rather, the proper analysis is whether the requested discovery would "significantly alter the quantum of proof" by, in this scenario, "cast[ing] doubt on the admissibility of evidence." Fed. R. Crim. P. 16(a)(1)(E); Local Rule 116.2; *Goris*, 876 F.3d at 45. If the answer to that question is yes, the government must produce the discovery. *Id*.

Here, Mr. Kiejzo has made a sufficient showing, to the extent possible with the materials available to him, that this information is material to preparing Mr. Kiejzo's defense and it is exculpatory under Fed. R. Crim. P. 16(a)(1)(E), Local Rule 116, and *Brady*, 373 U.S. at 87. The materials available to Mr. Kiejzo suggest that there was, at minimum, a collaboration between the United States and the FLAs in the investigation in this case. *See* Motion to Compel, 4-7, 10-12. Mr. Kiejzo is entitled to discovery that further reveals the level of collaboration between the United States and the FLAs because it goes to the heart of whether the FLAs' investigations involved searches within U.S. territory, and whether the FLAs acted with U.S. agents, at the behest of U.S. agents, or as agents for their American counterparts, such that there was a "joint venture" or that it constituted activities which would shock the conscience in violation of the Fourth Amendment. *See United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012). This information begins with naming the FLA that seized the computer servers hosting Websites 2 and 3.

The Magistrate's assumptions that led him to conclude otherwise were erroneous. Specifically, the Magistrate posited that "if U.S. agents had participated in, for instance, the seizure of the websites server(s), common sense suggests that a FLA tip would have been unnecessary to alert agents of the activities of the 96 IP address; rather, U.S. agents would have possessed such information." Exhibit N at 7. Similarly, the Magistrate reasoned that "it seems equally unlikely that U.S. agents directed an investigation into what IP addresses accessed the websites, since, as noted in the affidavit, the hidden service websites on the TOR network are accessible globally and users may be located anywhere in the world, not necessarily or only in the U.S." *Id*. A recent case from the Northern District of Illinois, *United States v. Mitrovich*, 458 F. Supp. 3d 961 (N.D. Ill. 2020), reveals the flaws in the Court's reasoning here.

In *Mitrovich*, the FBI began investigating a child pornography website in 2014. *Id*. at 963. Sometime that year, the FBI "obtained the ability to identify IP addresses associated" with the website, and learned that the website was hosted in the Netherlands, with the head administrator residing in Australia. *Id*. After the FBI shared that information with Australia, law enforcement agencies from Australia and New Zealand seized control of the website, operated it undercover, and shared backup copies of the website with the FBI. *Id*. As part of its investigation, the Australian and New Zealand authorities uploaded a hyperlink onto the website that, when clicked, allowed them to capture the clicker's IP address, which would have otherwise been concealed by Tor. *Id*. One particular user – known as "cyberguy" – clicked on the hyperlink, thereby revealing his IP address, which was located in the United States, to the Australian and New Zealand authorities. *Id*. Australia and New Zealand sent the IP address to the FBI, which then obtained records from Comcast to identify the physical address associated with the IP address. *Id*. The FBI subsequently

obtained a search warrant for that address – the defendant's home – and discovered child pornography materials therein. *Id*.

The facts in *Mitrovich* demonstrate how, contrary to the Magistrate's conclusions, a United States law enforcement agency in fact could *and did* participate in the seizure of a website server, but was not in possession of a particular user's IP address. The facts also demonstrate that while U.S. agents may not necessarily direct an investigation into one particular IP address, a U.S. law enforcement agency could be engaged in a joint venture to uncover IP addresses within the United States.

In *Mitrovich*, the court found that the defendant had made a prima facie showing that the joint venture doctrine applied, based principally on an FBI memorandum describing the investigation. *Id*. at 965-66. The court held that the motion to compel could not be denied "based on the Government's submission that the exclusionary rule [did] not apply to the investigatory conduct of [Australian and New Zealand authorities]." *Id*. at 966; *see also United States v. Budziak*, 697 F.3d 1105, 1113 (9th Cir. 2012) (holding that it was "an abuse of discretion for the district court to deny . . . discovery on [a software program developed by the FBI that allowed it to see what files particular users were downloading]," reasoning that "criminal defendants should not have to rely solely on the government's word that further discovery is unnecessary . . . "). Mr. Kiejzo has made a similar showing in his Motion to Compel and is therefore entitled to the requested discovery. *See* Motion to Compel, 4-7, 10-12.

Discovery Requests #6-7*: The substance of the notification by the "FLA" to U.S. law enforcement regarding the identification of the IP address in this case, as referenced in ¶¶ 31-32 of the affidavit, including but not limited to:*

a. the author of the "FLA" notification;

b. the identity of the "U.S. Law Enforcement" agency which received the notification and the recipient;

c. the complete content of the notification, including information on tactics and/or techniques utilized by the "FLA" to determine the identity of the IP address accessing the website;

d. any and all descriptions and/or identifications of Website 2 provided by the "FLA" in its tip to the U.S.;

e. the "further documentation" regarding Websites 2 and 3 provided by the FLA as referenced in ¶¶ 31-32 of the affidavit.

Discovery Request #16*: Any and all cover sheet(s), correspondence, and/or index list documenting the totality of "tip" and/or "notification" information provided by the FLA.*

Items #6-7(a)-(b) are relevant to whether the material was produced and provided in connection with a joint or coordinated effort between the United States and foreign law enforcement agencies and must be produced for the same reasons described above.

With respect to items #6-7(c)-(e) and #16, the defense has received three seemingly incomplete sets of heavily redacted documents. The first set of documents contains two undated single-page reports that allege an IP address was twice "used to access online child sexual abuse and exploitation material" on May 12, 2019, seventeen minutes apart. *See* Exhibit G. The second set is a single letter from [redacted] to the FBI – addressed to an unnamed person/unit within the FBI, and authored by an unnamed person/unit in [redacted] – that does not reference the two single-page [redacted] reports by either date or reference number or reference the IP address named in those two reports. *See* Exhibit H. The third set contains two single-page intelligence reports from the [redacted] that name the two websites but have no correlation to the IP address or the May 2019 date mentioned in the tip. *See* Exhibit I.

These documents are not only not responsive to Mr. Kiejzo's request but also suggest that more documentation exists and has been withheld. Agent Moynihan's affidavit specifically states

that the FLA – now identified as [redacted] – "notified U.S. law enforcement that the FLA had determined that on May 12, 2019… [the IP address] was used to access online child sexual abuse and exploitation material **via a website that the FLA named and described** as Website 2 [and 3]." Exhibit F at ¶ 31, 32. The affidavit also refers to other "documentation naming the website[s]." *Id*. None of the documents provided so far have connected the website by name with the specific IP address and the specific date mentioned in the affidavit. At the hearing, the defendant pointed out specific redactions and missing links in the chain between these sets of documents. The Magistrate acknowledged that there appeared to be a discrepancy, and urged the government to consider un-redacting the documents related to the tip, but did not explicitly order the government to do so. *See* Exhibit L at 30, 32-33. As of today's date, the government has not provided un-redacted versions of Exhibits G-I.

The Magistrate is correct that the documentation sought by the defense relates to Mr. Kiejzo's potential *Franks* motion. Exhibit N at 8-9. However, the Magistrate's finding that Mr. Kiejzo was not entitled to this discovery because he had not made the "substantial preliminary showing" required to obtain a *Franks* hearing was erroneous for two reasons. *See id*., 8.

First, at least one case from this district suggests that the defendant does not need to make a "substantial" showing to obtain discovery prior to a *Franks* hearing. In *Jordan*, 2010 WL 625280, at *3-4, the court held that when a defendant seeks discovery to mount a *Franks* challenge, the production of the discovery sought should await an "initial showing" of inaccuracies in the affidavit that, if omitted, would preclude a probable cause finding. In contrast to the Magistrate's order, that court did not find that a "substantial" showing was necessary to obtain discovery that would support a *Franks* motion. *Id*.

Second, under either standard, Mr. Kiejzo has sufficiently shown that there are material inaccuracies and omissions in the affidavit. Principally, Agent Moynihan misrepresented the nature and origin of the tip from [redacted]. In the affidavit, Agent Moynihan stated that U.S. law enforcement was notified by an FLA that a specific IP address had accessed child sexual abuse material on May 12, 2019 at two specific times *via websites that were named and described as Websites 2 and 3*. Exhibit F at ¶ 31-32. From the documents provided to the defense, it is clear that Agent Moynihan's statement in the affidavit is inaccurate. Rather than repeating the tip verbatim, Agent Moynihan added language and omitted information to make it appear to the Magistrate that U.S. law enforcement had more evidence of criminal activity than it actually did. For example, Agent Moynihan omitted from the affidavit the now-apparent fact that U.S. law enforcement had no evidence that an internet user associated with that IP address had created an account on either website or logged into either website. *See* Exhibit L at 41-42. Agent Moynihan also omitted from the affidavit the fact that U.S. law enforcement had no evidence of what, if anything, was actually "accessed", viewed, or downloaded on that date at those times.

Agent Moynihan also made a number of misrepresentations regarding the reliability of the tip. In the affidavit, Agent Moynihan stated that the FLA that provided the tip ([redacted]) was a "national law enforcement agency of a country with an established rule of law." Exhibit F at ¶ 33. Agent Moynihan further stated that the FLA advised U.S. law enforcement that it "had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address information." *Id*. Finally, Agent Moynihan claimed that prior tips from the FLA had led to an arrest, the rescue of children subject to abuse, and the seizure of evidence. *Id*. at ¶ 34. However, Agent Moynihan failed to include the fact that there was not just one FLA involved in obtaining the IP address, but two – from two wholly different countries –

and thus that the government's representations and assurances in the affidavit about either the scope of U.S. involvement or the denial of interaction with any computer in the U.S. applied only to the FLA that provided the tip to U.S. law enforcement (again, [redacted]). Agent Moynihan did not make this distinction in the affidavit, and instead created the impression that the tip and the source of that tip both originated from the same, reliable FLA. This impression was misleading and inaccurate. Notably, the government has made no similar such assurances or representations about the lack of U.S. involvement in the seizure of the server, or the absence of coordination or collaboration with the seizing FLA. Neither has the government made any similar such assurances or representations about the deployment of investigative techniques by the seizing FLA, with or without U.S. involvement, to interfere with, access, search, or seize any data from any computer in the U.S.

These inaccuracies about the nature and reliability of the tip go to the heart of the probable cause analysis. The tip from the FLA was the only allegation of criminal activity in the entire affidavit. It was also the only piece of information that created any nexus to Mr. Kiejzo and his home. If these inaccuracies were corrected, and if the omitted information were added, the affidavit would not establish probable cause to search Mr. Kiejzo's home. This "initial showing" is sufficient to warrant further discovery prior to a *Franks* hearing.

> ***Discovery Request #8****: Any record of the investigative technique(s) utilized by the FLA with respects to the "notification(s)" described in ¶¶ 31-33 of the affidavit.*

The government continually refuses to provide any information regarding the investigative technique utilized by [redacted] or unnamed FLA to identify the IP address in this case, and the investigative technique, if different, to link the IP address to the target websites. The government's refusal to provide such information rests on their assertion that the investigative technique is not relevant to any potential basis for suppression and is not otherwise discoverable. However, the

manner in which the IP address was identified and de-anonymized – whether it was through the use or deployment of a network investigative technique ("NIT"), or some other means – is material because it is crucial to determining whether a search occurred.

The Magistrate Judge rejected Mr. Kiejzo's argument that he is entitled to this discovery as mere speculation. However, an expert declaration submitted in a case virtually identical to Mr. Kiejzo's suggests that the specific IP address could not have been identified without running a NIT or, in the alternative, an error-prone traffic analysis technique. *See* Declaration of Steven Murdoch at ¶ 22-32, *United States v. Sanders*, No. 20-cr-00143 (E.D. Va. Sept. 17, 2021), ECF No. 464-2, attached as Exhibit M. Either scenario would significantly undermine the veracity of the affidavit and its probable cause showing. The deployment of a NIT would constitute an unlawful warrantless search, the results of which could not be considered in Agent Moynihan's affidavit. *See e.g. United States v. Anzalone*, 208 F. Supp. 3d 358, 366 (D. Mass. 2016). The use of a NIT would also reveal a substantial misrepresentation in the affidavit, which relies on Agent Moynihan's assurance that no computer in the United States had been searched. Exhibit F at ¶ 33. Alternatively, the fact that the traffic analysis technique described in Professor Murdoch's declaration is inherently error-prone would undermine the strength and reliability of the tip such that no magistrate, had he or she been aware that this technique was used to obtain the IP address, would find there was probable cause. *See* Exhibit M at ¶ 22-32.

The technique used to identify the IP address is also material to whether, and to what extent, U.S. law enforcement directed, assisted, and/or participated in the investigation as outlined in Discovery Requests #3-4. In the affidavit, Agent Moynihan claimed that U.S. law enforcement had not participated in the investigative work "through which FLA identified the IP address information provided by FLA." Exhibit F at ¶ 33. However, as argued above, Agent Moynihan

deliberately obscured the fact that there were two distinct FLAs, from two different countries, involved in obtaining the IP address. The Agent's assurances that U.S. law enforcement did not "participate" only applied to [redacted], not to the as-yet unnamed FLA. The government has made no such assurances as to the unnamed FLA.

Finally, the government's assertion that Mr. Kiejzo is not entitled to this discovery simply because it has determined it is not relevant cannot preclude production of the requested information. *See Mitrovich*, 458 F. Supp. 3d at 966; *Budziak*, 697 F.3d at 1113.

> ***Discovery Request #9***: *Any information, document, memorandum, and/or agreement addressing whether the FLA provided the information regarding the IP address in this case as part of a coordinated initiative or program with U.S. law enforcement.*

The government's response to this discovery request did not address whether the U.S. was involved in any investigative phase of this operation, whether the U.S. provided or requested information during the course of the operation, or whether it was conducted pursuant to an understanding, memorandum, collaboration, cooperation, mutual assistance treaty, and/or agreement between U.S. law enforcement and the FLA, or at the behest, direction, and/or benefit of the U.S. The requested discovery is material and potentially exculpatory, and the Magistrate's finding to the contrary is erroneous, for the same reasons described above in Discovery Requests #3-4. The requested material relates to the existence of a joint venture between the United States and the FLAs, which is central to the Fourth Amendment issues in this case.

> ***Discovery Request #10***: *Complete copies of the "advisements" by the FLA to U.S. law enforcement regarding the "independent investigation" and "investigative work through which the FLA identified the IP address information" in this case, as referenced in ¶ 33 of the affidavit.*

Mr. Kiejzo is entitled to the requested discovery for the same reasons outlined in Discovery Requests #s 3, 4, and 8. The Magistrate Judge denied this request, finding the Mr. Kiejzo's

argument to be speculative. For the same reasons outlined above in Discovery Request #s 3, 4, and 8, this finding was erroneous and should be reversed by this Court.

> ***Discovery Request #13***: *The name of the "Operation," "Task Force," "Initiative," and/or organizing group assigned by the FLA to the investigation in this case, and the name of "Operation," "Task Force," "Initiative," and/or organizing group assigned by the FBI to the investigation in this case, if different.*
>
> ***Discovery Request #14***: *The specific case FBI ID and/or serial number assigned to the Defendant's case.*

The discovery requested in #13 and #14 is relevant for the reasons outlined in the Motion to Compel. Specifically, the discovery relates to the scope of the operation, the nature of any joint investigation and/or coordinated steps taken by different law enforcement agencies, and the membership(s) and/or role(s) of various law enforcement agencies and actors. To the extent that the Magistrate rejected Mr. Kiejzo's request on the basis that he failed to make a showing of a joint venture, Mr. Kiejzo refers to his arguments above in Discovery Requests #3-4 as to why that finding was erroneous.

Additionally, the Magistrate rejected Mr. Kiejzo's argument "that names and numbers assigned to the case are material to defending this case" without acknowledging or referencing Mr. Kiejzo's showing that [redacted] reports in this case appear to be two of many reports that are part of an as-yet unnamed operation that resulted in the identification of multiple IP addresses at the same time. *See* Exhibit N at 10; Motion to Compel, 2 fn. 3. In fact, defense counsel has reason to believe that the name of this overarching operation has been disclosed in other cases similar to Mr. Kiejzo. *Id*. at 2 fn 3 and 22. Although those cases are subject to restrictive protective orders, the facts that are available are strikingly similar to those in Mr. Kiejzo's. *See* Motion to Compel, 2 fn. 3. The name of the operation and the case number assigned to Mr. Kiejzo's case are relevant to the scope of this operation and are, for the reasons outlined above, material and exculpatory.

The Magistrate's finding that Mr. Kiejzo is not entitled to the discovery to support a *Franks* challenge is erroneous for the reasons stated in Discovery Requests #6-7 and #16.

> ***Discovery Request #15****: Any record of action taken in response to the FLA notification by U.S. Law Enforcement agencies, including but not limited to copies of subpoenas and supporting materials (including spreadsheets, charts, lists, and/or other documents) sent to internet service providers, as referenced in ¶¶ 3 and 39 of the affidavit; and copies of returns to such subpoenas.*

As outlined in the Motion to Compel, the government provided a half-page document with subscriber information for a Verizon account associated with the target IP address in response to Mr. Kiejzo's request. *See* Exhibit K, Verizon Document. However, there is a significant discrepancy between this response and the information included in the affidavit. The affidavit states that "an administrative subpoena was issued to Verizon Fios for information related to [the IP address] on the following dates and times: May 12, 2019 at 19:10:51 UTC and May 12, 2019 at 19:27:24 UTC, respectively." Exhibit F at ¶ 39. The document produced by the government references customer information for a total of 10 months, not just those two dates. *See* Exhibit K. The Magistrate's ruling on this issue was that this discrepancy "is not significant." Exhibit N at 10-11. Mr. Kiejzo respectfully submits that the discrepancy highlights a misstatement in the affidavit that directly relates to the only link between the alleged criminal activity and Mr. Kiejzo's home.

> ***Discovery Request #17****: With respect to the notification by the FLA to U.S. law enforcement:*
> *a. whether, and how, the FLA determined that the defendant's IP address accessed and/or visited a specific portion of Websites 2 and/or 3, and, if so, what specific portion of Websites 2 and/or 3 was accessed and/or visited;*
> *b. the number of tips provided by the FLA to U.S. law enforcement pursuant to its investigation under the* [redacted] *as referenced in its September 16, 2019 letter;*
> *c. the number of websites identified by the FLA to U.S. law enforcement pursuant to its investigation under the* [redacted]*;*
> *d. the number of IP addresses identified by the FLA to U.S. law enforcement pursuant to its investigation under the* [redacted]*.*

The Magistrate denied Mr. Kiejzo's request as to #17(a) because the government asserted that "it is not in possession of information showing which portions of Websites 2 and 3 the 96 IP address accessed." Exhibit N at 11. However, the government made no such assertion regarding the technique used by the FLA to identify the IP address that accessed the websites. The government must produce that information for the same reasons outlined in Discovery Request #8. Additionally, the government's assertion does not relieve it of its constitutional obligations under *Brady* to disclose exculpatory evidence. *See also Kyles v. Whitley*, 514 U.S. at 437.

With regard to Request #17(b)-(d), the requested discovery is material to the scope of the investigation, the method and reliability of the FLA's identification of IP addresses, websites, and users' activity, and the specificity of the FLA tip as to Mr. Kiejzo. The numbers of tips and IP addresses provided by the FLA are especially relevant considering the nearly identical and/or substantially similar timeframes and tip language for each IP address. Disclosure of this information is also relevant to the capability of the FLA and the methods it used to identify users' conduct and activity on a website, and to unmask individual IP addresses related to specific conduct and activity on a website. As this discovery relates to the existence of a joint venture, it must be produced for the same reasons outlined in Requests #3-4. As it relates to the FLA's potential use of a NIT, the discovery must be produced for the same reasons outlined in Request #8. The Magistrate's ruling that Mr. Kiejzo failed to make a sufficient showing to warrant discovery for a *Franks* challenge is erroneous for the reasons outlined in Requests #6-7.

CONCLUSION

The Magistrate Judge's order denying Mr. Kiejzo's Motion to Compel was erroneous and contrary to law. This Court should set aside the order pursuant to Fed. R. Crim. P. 59(a).

Respectfully submitted,
VINCENT KIEJZO
By His Attorney,

/s/ Sandra Gant
Sandra Gant, B.B.O.# 680122
Federal Public Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

/s/ Caitlin Jones
Caitlin Jones, MN ID # 0397519
Federal Public Defender Office
51 Sleeper Street, 5th Floor
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I, Sandra Gant, hereby certify that this document filed through the ECF system will be sent electronically to the registered participant(s) as identified on the Notice of Electronic Filing (NEF) on October 18, 2021.

/s/ Sandra Gant
Sandra Gant